Cassandra Crossing/ Tor, lezioni di guida—3

(98)—La difesa dell'anonimato in rete e l'autotutela sono alla portata di tutti: terzo step nell'utilizzo di Tor, alla conquista di…

Cassandra Crossing/ Tor, lezioni di guida—3

Figure 1:

(98)—La difesa dell'anonimato in rete e l'autotutela sono alla portata di tutti: terzo step nell'utilizzo di Tor, alla conquista di Privoxy. Pochi clic per un nuovo mondo.

31 ottobre 2007—Fino ad ora abbiamo considerato l'uso di Tor come applicazione isolata, e descritto e risolto alcuni problemi elementari che possono compromettere il livello di privacy ed anonimato raggiungibile con il suo uso.

Oggi affronteremo il problema da un punto di vista diverso: porremo al centro dell'attenzione non i software che girano all'interno del PC, ma piuttosto il flusso di informazioni che si muove tra il PC ed internet, indipendentemente dai programmi che lo generano.

Chi seguendo queste chiacchierate avesse installato Tor per la prima volta, si sarà probabilmente accorto che anche i siti di download più popolari di Tor come ad esempio quello di EFF propongono, accanto ai file di installazione di Tor, alcuni bundle, che contengono oltre a Tor anche altri programmi, tra cui immancabilmente Privoxy.

Che cos'è Privoxy?

Questa è facile. Privoxy è un proxy filtrante.

E perché ne abbiamo bisogno? Tor non è già lui un proxy?

Facciamo un passo indietro. Tra il nostro PC ed i server cui accediamo via Internet esiste un flusso di informazioni fatto di richieste e risposte alle richieste. Senza perdita di generalità possiamo continuare a pensare alla normale navigazione web fatta con un browser come Firefox. Usare Tor durante la navigazione "devia" questo flusso e lo costringe a fare delle tappe intermedie attraverso la rete dei router Tor prima di raggiungere la destinazione finale; questi passaggi intermedi rendono difficile correlare le richieste che raggiungono i server web e le relative risposte con l'utente che le ha generate.Continuando ad utilizzare il modello a flusso di informazioni possiamo evidenziare due tipi di rischi per la privacy.

Il primo ed il più banale è quello di una parziale "deviazione" di questo flusso, normalmente incanalato nella rete Tor attraverso il nostro proxy Tor locale, che faccia uscire direttamente alcune informazioni su Internet, compromettendo così la privacy della navigazione.

Questo esempio non è scelto a caso, perché è stato un problema delle prime release di Tor.In pratica, quando usiamo Tor diciamo al nostro browser "usa Tor come proxy socks" ovvero "fai passare tutto attraverso Tor".

Alcuni browser ed applicazioni Internet, certi più di altri, possono non onorare completamente questa richiesta. La prima operazione che il browser deve compiere prima di stabilire la connessione che gli abbiamo richiesto è quella di prendere il nome del server contenuto nell'indirizzo della pagina richiesta e tradurlo nell'IP verso cui aprire la connessione.

Per far questo deve aprire una diversa connessione verso un server particolare di cui già conosce l'indirizzo (il server DNS) al quale inviare il nome dell'host e riceverne il corrispondente IP. In alcuni casi questa nuova richiesta non veniva fatta passare da Tor e quindi diventava banale per un attaccante correlare l'IP di chi aveva appena richiesto l'indirizzo di un certo sito con il richiedente di una connessione anonima che arrivava immediatamente dopo allo stesso sito.In certi casi (tipicamente bachi del browser) queste richieste potevano passare all'esterno di Tor.

Il secondo, e ancor più grave problema, è quando nel flusso di informazioni passano dati che possono far identificare l'utente. Le connessioni fatte attraverso Tor sono normali sessioni HTTP od HTTPS. Il server a cui vengono effettuate le richieste, e nel caso che si usi l'HTTP non criptato anche il router Tor di uscita e chi è in grado di sniffare il traffico, possono intercettare e raccogliere tutto quello che viene trasmesso.

Se l'utente accede a delle informazioni su un suo sito personale ma gestito da un provider, o per distrazione invia dati personali riempiendo un form, magari con il numero della sua carta di credito, il suo anonimato viene irrimediabilmente compromesso.Il problema può essere risolto, od almeno grandemente mitigato, installando (in termini tecnici: concatenando) un secondo proxy a Tor, Privoxy appunto.In questo caso il browser non manda più i dati direttamente a Tor, ma li invia a Privoxy, che può esaminarli ed eventualmente modificarli prima di inviarli in Rete; può così ad esempio rimuovere il nome ed il cognome dell'utente che per qualsiasi motivo fossero finiti nel flusso dei dati.

Analogamente può essere configurato per intercettare la pagina in arrivo da Tor e rimuovere tutti gli script Javascript, in modo che anche se il browser fosse impostato per eseguirli il problema sia risolto "alla radice".

Se installate Tor con il bundle dal sito di EFF vi ritroverete con Privoxy già installato e configurato, ed avrete anche Torbutton ed un pannello informativo molto utile che si chiama Vidalia, che permette di visualizzare, anche geograficamente, il routing di Tor attraverso la Rete.

Privoxy ha un dettagliatissimo pannello di controllo raggiungibile dall'indirizzo http://config.privoxy.org (indirizzo che usando Privoxy non è su Internet ma sul vostro pc!)
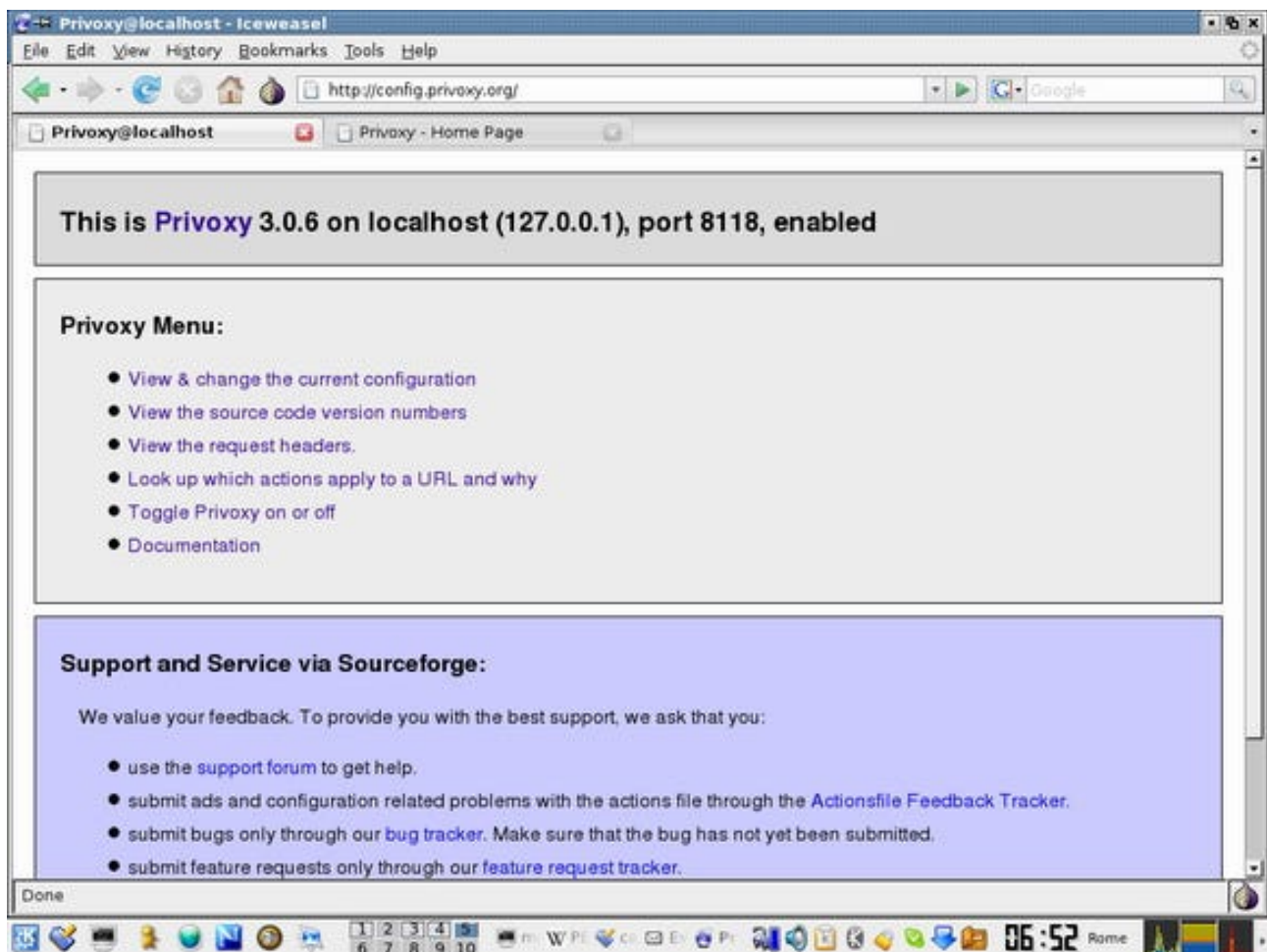
Figure 2:

da cui è possibile verificare lo stato del proxy, controllare il dettaglio delle azioni compiute su una certa pagina, configurare azioni predefinite o crearne di nuove, abilitare o disabilitare opzioni.
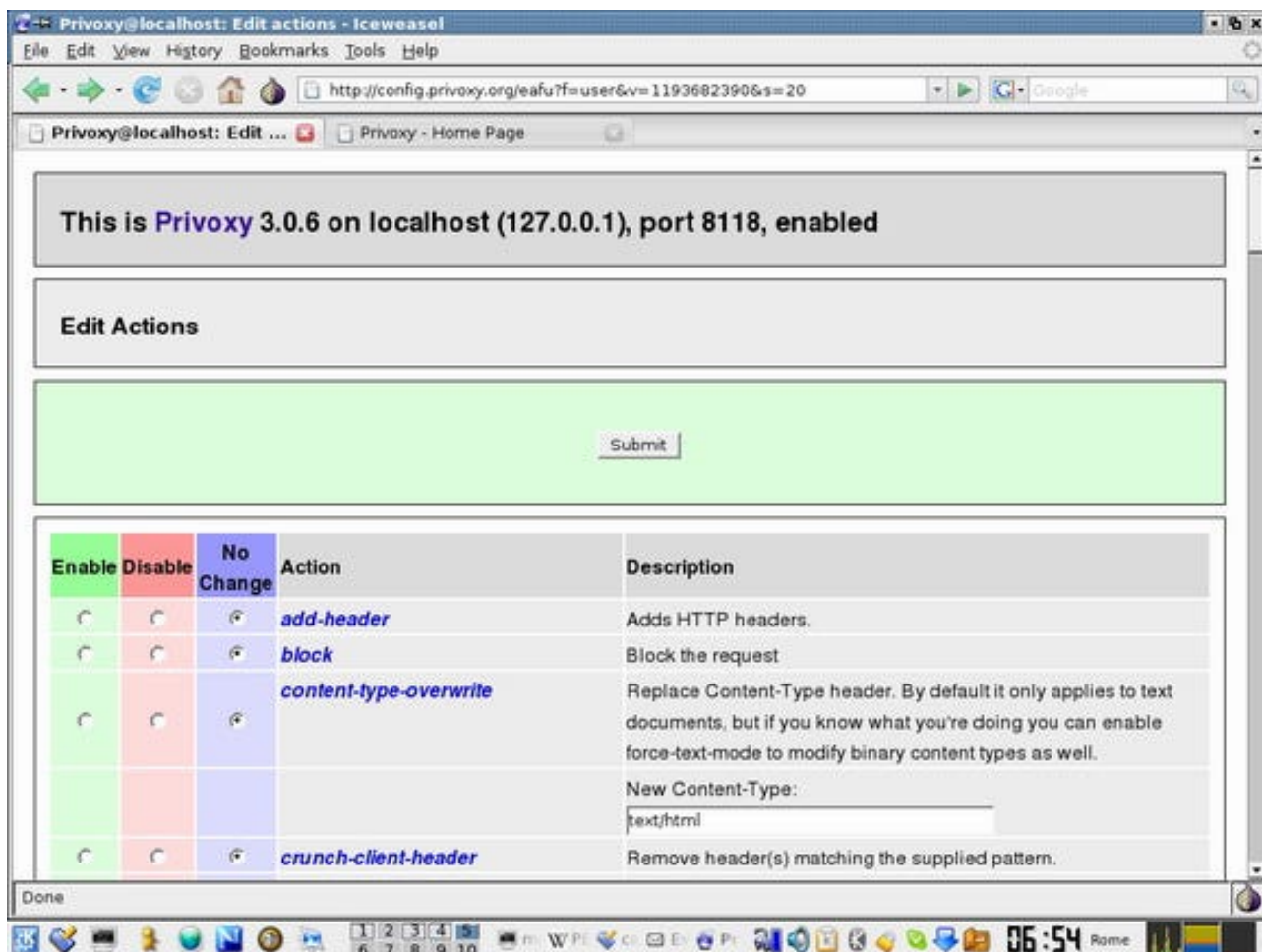
Figure 3:

ed infine accedere alla documentazione. Un esercizio molto interessante che consiglio a tutti è di creare ed abilitare un filtro che sostituisca sistematicamente una parola nelle pagine in arrivo. Nel file di configurazione ce ne è uno predefinito (solo da abilitare).Possono essere eseguite anche altre azioni più sofisticate come rimuovere le immagini provenienti da siti di pubblicità basandosi sulla loro dimensione in pixel, oppure sostituire i gif animati con il loro primo fotogramma, per evitare quella pagine frenetiche piene di animazioni.

Infine vale la pena di ricordare che, dopo averlo installato, anche un proxy filtrante funziona comunque molto meglio se c'è qualcosa collegato tra la tastiera e la sedia; niente può sostituire un po' di attenzione e di accortezza da parte dell'utente.

Oggi abbiamo individuato una soluzione efficace ed utilissima ad una parte degli errori e delle distrazioni che si possono commettere navigando anonimamente in Rete con Tor; la prossima volta parleremo dell'installazione di un server Tor.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 30, 2023.

Canonical link

Exported from Medium on August 27, 2025.